RECOMENDAÇÕES PARA O EXERCÍCIO DE FUNÇÕES EM TRABALHO REMOTO

Segurança e Proteção de Dados

05 de novembro de 2020

1. Recomendações gerais de segurança

a) Discuta com a sua equipa as formas e procedimentos a adotar em trabalho remoto, incluindo a distribuição de tarefas, prazos e canais de comunicação;

b) Utilize prefencialmente os computadores da UCP (em vez do computador pessoal) sempre que possível, a menos que o seu PC tenha sido devidamente preparado pelos serviços de IT da UCP; utilize apenas software e equipamentos referenciados pela UCP;

c) Antes de começar o trabalho remoto, esteja familiarizado com os equipamentos, procedimentos e políticas da UCP; certifique-se que compreende o equipamento e os procedimentos e, em caso de necessidade, procure apoio e informações junto dos serviços de IT;

d) O acesso remoto deverá ser seguro através de VPN;

e) Crie passwords fortes e não as escreva, memorize-as;

f) Sempre que possível, não misture atividade de laser e particulares no mesmo dispositivo que utiliza para prestar o seu trabalho; Preferencialmente seja o único utilizador do PC em que trabalha; Proteja o seu equipamento e ambiente de trabalho remoto, não permita a outros membros da família o acesso aos seus equipamentos

g) Ligue-se à internet através de redes seguras; não use redes públicas. A maioria dos sistemas wi-fi em casa encontra-se devidamente protegida, mas algumas redes mais antigas poderão não estar. Certifique-se dessa proteção, na medida em que, sem uma ligação segura, pessoas nas proximidades podem ter acesso à sua informação. A solução é ativar a criptografia caso

ainda não tenha sido feita e / ou adotar uma implementação recente. Observe que esse risco é um pouco atenuado com o uso de uma conexão segura com o escritório.

h) Evite a troca de informações contendo dados pessoais ou informações confidenciais (via email) através de ligações não seguras;

i) Na medida do possível, para partilha de documentos, utilize os recursos da intranet ou das áreas de partilha (pastas) criadas para o efeito e em uso na UCP;

j) O seu computador deverá ter um sistema operativo atualizado e ter instalado um antivírus também ele atual;

k) Ative o seu bloqueio de teclado e de ecrã ao final de um tempo de inatividade;

l) Não partilhe os links nem as passwords de reuniões virtuais com pessoas que não sejam os participantes nem através de redes sociais ou outros canais públicos.

m) Seja particularmente cuidadoso e esteja com atenção redobrada a emails que façam referência ao COVID-19, pois podem ser tentativas de phishing; caso tenha dúvidas sobre a origem ou a legitimidade de um email entre em contacto com os responsáveis pelos sistemas de IT;

2. Ataques de phishing ligados ao COVID 19

a) É importante que aumente a consciência sobre as questões relacionadas com a segurança digital pois a tendência é a de aumento dos ataques de phishing.

b) Na situação atual, deve suspeitar de qualquer email solicitando a

verificação que lhe exija verificação ou renovação de credenciais, passwords, etc… mesmo que lhe pareça de uma fonte segura; a UCP não solicita o envio de passwords por email.

c) Não clique em links nem abra quaisquer anexos suspeitos e verifique a legitimidade da fonte.

d) Suspeite de emails de remetente que não conhece especialmente se lhe é pedido para licar em links ou abrir anexos. Mensagens enviadas de pessoas que conhece mas que contêm mensagens ou pedidos fora de comum; faça essa verificação por telefone, se possível; desconfie de emails que criam uma imagem de urgência na resposta.

e) Não forneça informação ou dados pessoais através de email, mesmo que lhe pareça de uma fonte legítima e fidedigna; certifique-se que os mesmos lhe estão a ser efetivamente solicitados;

3. Proteção de dados pessoais

a) Relativamente à forma como os dados pessoais estão a ser objeto de tratamento, os colaboradores e docentes não poderão criar bases de dados nos seus computadores nem gravarem bases de dados retiradas dos sistemas e repositórios da UCP nos seus computadores ou pens;

b) Não deverão ser criadas listagens nem enviadas bases de dados pessoais por email.

c) A consulta, preenchimento, alteração, modificação e correção das bases de dados devem ser feitas no repositório formal respetivo (explo: SOPHIA, ABW, CRM);

d) A retirada de listas para o seu computador pessoal sem os procedimentos

de segurança adequados coloca em risco as pessoas, a confidencialidade, privacidade e integridade dos seus dados;

e) A Universidade possui mecanismos que permitem aos utilizadores a consulta e a partilha de bases de dados de forma segura.

f) Sempre que possível anonimize ou pseudominize os documentos de trabalho com bases de dados, e apague os dados de que não precisa para a execução da tarefa em questão.

g) Não partilhe documentos contendo dados pessoais nas plataformas de comunicação a distância (zoom, teams, etc)

h) Se tiver mesmo de enviar documentos com dados, faça-o com encriptação, protegidos por password ou pseudonomizados de forma a aumentar o seu grau de segurança.

4. Reporte

a) Caso detete alguma atividade fora do comum ou suspeita reporte essa situação imediatamente através dos canais apropriados;

b) Caso exista alguma suspeita relacionada com violação de confidencialidade de documentos ou de privacidade de dados por favor observe as regras em vigor relacionadas com as situações de “data breach”;

c) Caso tenha alguma suspeita relacionada com a legitimidade ou fidedignidade de algum pedido, email, procedimento por favor entre imediatamente em contacto com as equipas de IT ou de proteção de dados;

5. Exceções

É preciso ter em atenção que existem casos devidamente definidos em que

não é possível:

a)Aceder à consulta da base de dados ou outras aplicações consideradas sensíveis fora do posto de trabalho físico;

b) Consultar, analisar ou proceder ao tratamento de informação reservada ou confidencial sempre que tal seja considerado violador das regras de segurança.

6. Conclusão

A Universidade contém mecanismos adequados de segurança informática e e procedimentos robustos que evitam ataques informáticos, no entanto há situações que dependem da adoção de comportamentos e do cumprimento de regras adequadas, contando com o contributo dos colaboradores e docentes.

A confidencialidade, integridade e segurança dos nossos documentos e dos nossos dados pessoais e dos nossos alunos e parceiros depende de si e do cumprimento dos procedimentos de segurança.

Não hesite em colocar questões aos serviços de IT ou de proteção de dados.

Por favor adote comportamentos responsáveis!